E-Book

Mit einer sicheren Identity lässt sich alles schützen

Die drei Prinzipien einer modernen Identity-Strategie

okta

Woran denkt man in Ihrem Unternehmen bei Identity-Management zuerst?

In den meisten Fällen kommt zuerst Sicherheit in den Sinn – und das aus gutem Grund. In einer von Anmeldedaten-Diebstahl und Phishing-Angriffen dominierten Bedrohungslandschaft ist die digitale Identität (Identity) der wichtigste Vektor für Angriffe auf kritische Netzwerke und vertrauliche Informationen. Deshalb muss die Identity im Mittelpunkt jedes zukunftsfähigen, umfassenden Sicherheitsansatzes moderner Unternehmen stehen.

Dennoch sind noch viel zu viele Unternehmen weit von einer solchen Strategie entfernt. Sie setzen weiterhin auf das inzwischen veraltete Paradigma des sicheren Perimeters und merken immer deutlicher, dass die klassischen, auf Netzwerke und Geräte ausgerichteten Sicherheitstools kaum vor raffinierten Identity-basierten Angriffen schützen und nicht genug Transparenz bieten, um aufgedeckte Risiken effektiv beheben zu können.

Definition einer modernen Identity-Strategie

Eine moderne Identity-Strategie bietet die unverzichtbare Transparenz für Ihre gesamte Identity-Landschaft und zeigt dabei Schwachstellen auf, damit Sie Ihre Sicherheitslage stärken und bei potenziellen Angriffen schnell und effektiv reagieren können. Zudem kann eine moderne Identity-Strategie starken Schutz bieten und gleichzeitig nahtlose Verbindungen und reibungslose User Experiences ermöglichen, die für den geschäftlichen Erfolg heute unverzichtbar sind.

In diesem E-Book erfahren Sie, warum die Sicherheit und Technologie von Unternehmen auf Identity-Management aufbauen muss. Die Schwerpunkte sind:

- Die Zunahme Identity-bezogener Bedrohungen
- Warum klassische Identity-Ansätze keinen ausreichenden Schutz bieten
- Die drei Prinzipien für die Einführung von modernem Identity-Management

okta

Die Fragmentierung der Sicherheitstechnologien in Unternehmen

In den vergangenen zehn Jahren hat sich der in Unternehmen eingesetzte Tech-Stack enorm verändert. In schneller Folge wurden Cloud-Dienste und SaaS-Anwendungen eingeführt. Gleichzeitig hat Remote-Arbeit unsere Arbeitsweise und Vernetzung grundlegend gewandelt. Da Unternehmen sich heute nur durch technische Innovationen von ihren Mitbewerbern absetzen können, ist es nicht mehr praktikabel, auf ein monolithisches Enterprise-Gesamtpaket eines einzigen Anbieters zu setzen. Erfolgreiche Unternehmen wissen, dass ihre Mitarbeiter- und Kunden-Technologien Flexibilität und hohe Leistung gewährleisten müssen. Um dies zu erreichen, setzen sie auf verschiedene Best-of-Breed-Lösungen.

Moderne Tech-Stacks sind extrem hochentwickelt – und extrem kompliziert. Das ständig wachsende Netzwerk aus Einzellösungen führt zu fragmentierten IT-Umgebungen, bei denen die Unternehmensressourcen (einschließlich Identities) über ein Dickicht aus isolierten Systemen, Anwendungen und Infrastrukturen verstreut sind.

Isolierte Technologien führen zu blinden Flecken bei der Sicherheit

Diese Fragmentierung geht mit erheblichen Sicherheitsrisiken einher. Sie führt zu einer wachsenden Angriffsfläche für potenzielle Angreifer, da Identities an verschiedenen Stellen isoliert sind, sodass der Diebstahl und die Ausnutzung von Anmeldedaten schneller übersehen wird. Gleichzeitig wird es für Security-Teams praktisch unmöglich, sich den umfassenden und detaillierten Überblick zu verschaffen, der für die Erkennung und Behebung von Schwachstellen und Risiken erforderlich ist.

Angreifer wissen, dass Identities in den meisten Unternehmen wachsende blinde Flecken bilden – und nehmen diese bevorzugt ins Visier. Laut dem Verizon Data Breach Report 2024, an dem Okta beteiligt war, wurden bei 80 % aller Kompromittierungen kompromittierte Identities missbraucht.
Noch beunruhigender ist jedoch, dass sehr viele Unternehmen in Bezug auf Identity-Risiken noch völlig unvorbereitet sind: Im Jahr 2024 dauerte es im Durchschnitt sage und schreibe 290 Tage, bis ein Data Breach erkannt und eingedämmt wurde.

okta

Ein neuer Ansatz für Identity-Management ist nötig

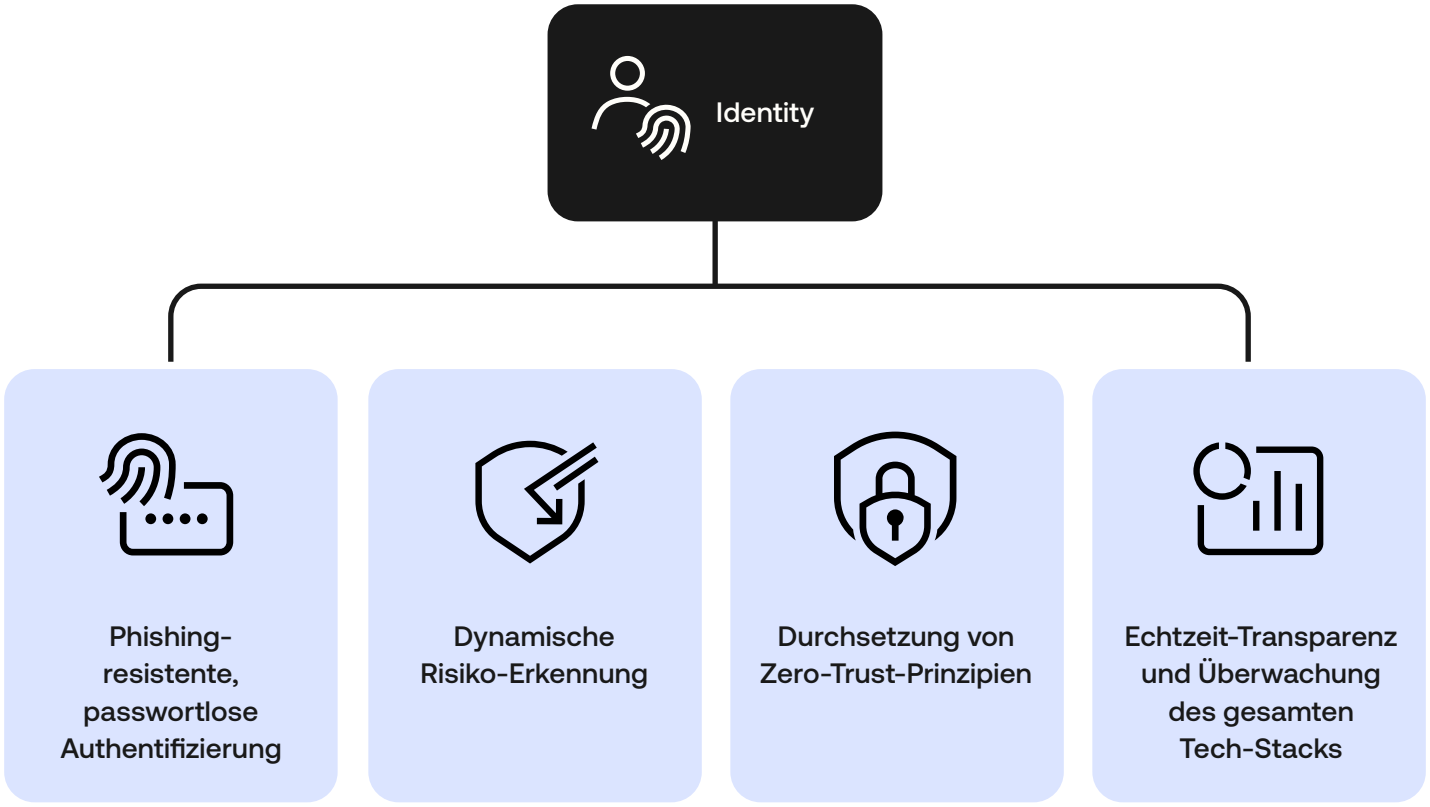
Jedes Unternehmen ist sich bewusst, dass Identity-Management für die Sicherheit eine wichtige Rolle spielt. Klassisch hat sie die Rolle eines Torwächters. Nur selten wird eine ebenso wichtige Rolle berücksichtigt: die des wesentlichen Elements für unternehmensweite sicherheitsbezogene Transparenz und Informationen.

Zum Beispiel setzen die meisten Unternehmen auf Identity, um den nahtlosen Zugriff mit sicherer Authentifizierung zu ermöglichen. Zur vollständigen Integration dieser Identity-Funktion in das Technologie- und Sicherheitsökosystem können sie die dynamische Risiko-Erkennung in Echtzeit sowie automatische Behebungsmaßnahmen einführen, um Angreifer zu stoppen, die sich mit gestohlenen Anmeldedaten erfolgreich authentifizieren konnten. Dies sind nur einige der Möglichkeiten, mit denen Identity einen zuverlässigeren und proaktiveren Ansatz unterstützt und Security-Teams hilft, die Sicherheitslage zu stärken.

Zentralisierung der Identities aus dem gesamten Sicherheitsökosystem

Wenn Unternehmen dieses Potenzial außer Acht lassen, ignorieren sie einen bekannten Fakt: Identity ist heute die am häufigsten attackierte Angriffsfläche, das häufigste Einfallstor für Angreifer und gleichzeitig der Bereich, in dem erfolgreiche Security-Teams Angriffe am einfachsten abwehren können.
Eine moderne Identity-Strategie hat das Potenzial, jede Komponente Ihrer Sicherheitsumgebung miteinander zu verknüpfen und dadurch den Schutz vor hochentwickelten und raffinierten Bedrohungen zu verstärken und zu vereinheitlichen.

Um dies zu erreichen, müssen Unternehmen besser – und auch aus strategischer Sicht – verstehen, was Identity ist und was sie leisten kann.



Ein genauerer Blick auf die Bedrohung

Angreifer vertrauen darauf, dass Unternehmen veraltete Identity-Ansätze nutzen. Bei fragmentierten IT- und Sicherheitsumgebungen sind wichtige Ressourcen, Anwendungen und Identities über verschiedene Systeme und Infrastrukturen verteilt, sodass Identity-basierte Angriffe leicht übersehen werden können. Die Konsequenzen können sich auf Unannehmlichkeiten beschränken – oder verheerend sein.

Manuelle Prozesse

Umständliche, zeitaufwändige und fehleranfällige Prozesse zur Berechtigungsverwaltung

Blinde Flecken

Unzureichender Überblick über die aktuelle Sicherheitslage des Unternehmens sowie über die Berechtigungen der einzelnen Benutzer für die verschiedenen Systeme und Anwendungen

Lange Reaktionszeiten

Verzögerte Reaktionen erleichtern Angreifern teure, verheerende Sicherheitsverletzungen, die Identity-bezogene Schwachstellen ausnutzen

Das Problem wird nicht verschwinden, sondern schnell immer größer werden. Wenn Anwendungen, Services und Benutzer KI einsetzen, lassen sich Identity-bezogene Risiken immer schwerer erkennen und abwehren. Erschwerend kommt hinzu, dass es bei Identity-basierten Angriffen nicht mehr nur um gestohlene Anmeldedaten geht. Durch Bedrohungen, die nach der Authentifizierung ansetzen (z. B. gestohlene Session-Cookies), wird die bereits komplexe Überwachung der Protokollinformationen auf verdächtige Aktivitäten noch komplexer. Außerdem besteht dauerhaft ein Risiko durch kapitalkräftige staatlich unterstützte Angreifer und schwer erkennbare Insider-Bedrohungen. Kurzum: Sie haben einen völlig unzureichenden Überblick darüber, wo die Risiken eigentlich sind – und welche Stoßrichtung sie haben.

80 %

Über 80 % aller Data Breaches werden von Identity-basierten Angriffen verursacht.

(Verizon)

180 %

Die Zahl Identity-basierter Angriffe ist im Jahresvergleich um 180 % gestiegen.

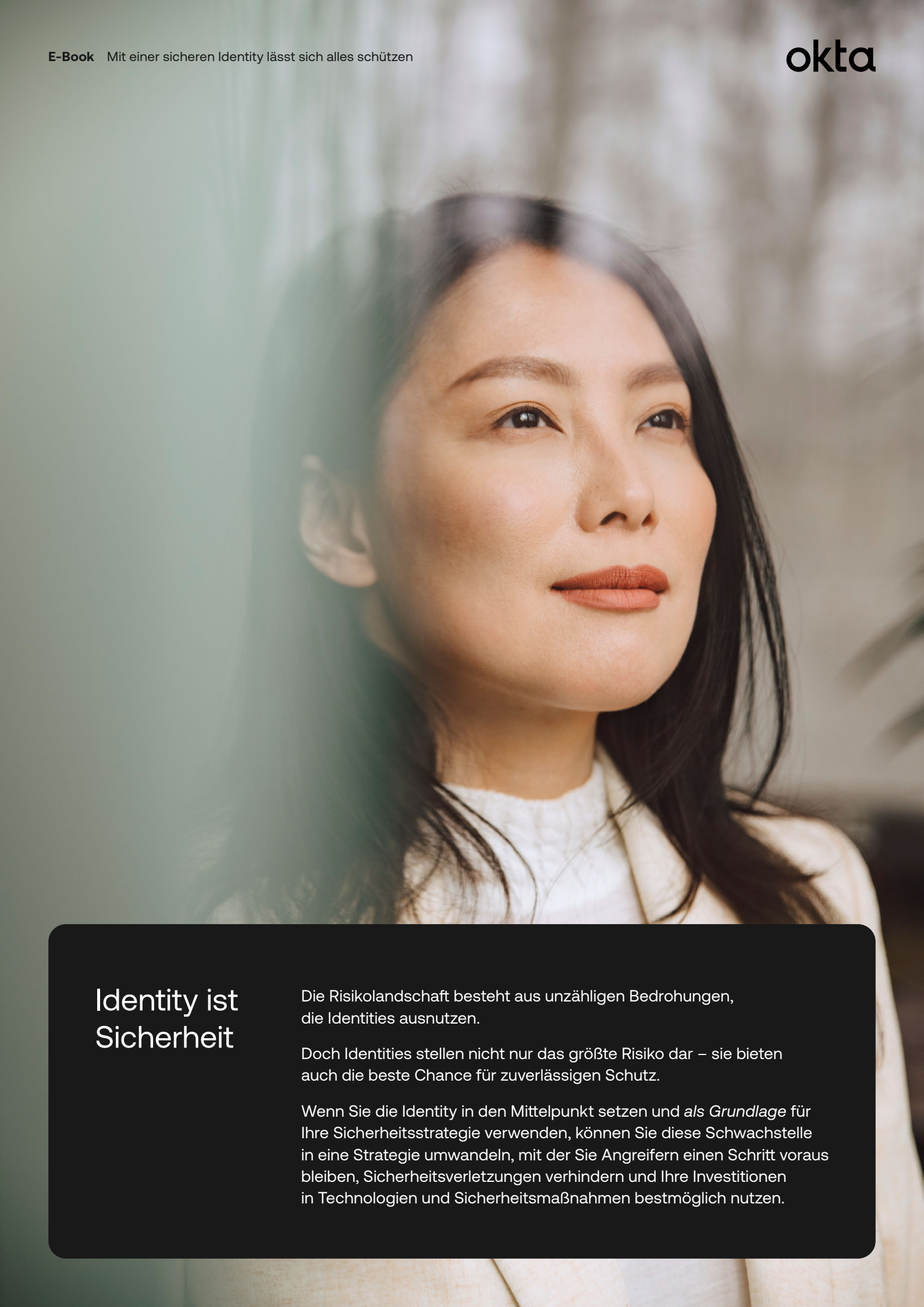
(Verizon)

1,9 Mrd.

1,9 Milliarden Session-Cookies wurden 2023 bei Mitarbeitern von Fortune 1000-Unternehmen gestohlen.

(Fortune)

okta



Identity ist Sicherheit

Die Risikolandschaft besteht aus unzähligen Bedrohungen, die Identities ausnutzen.

Doch Identities stellen nicht nur das größte Risiko dar – sie bieten auch die beste Chance für zuverlässigen Schutz.

Wenn Sie die Identity in den Mittelpunkt setzen und *als Grundlage* für Ihre Sicherheitsstrategie verwenden, können Sie diese Schwachstelle in eine Strategie umwandeln, mit der Sie Angreifern einen Schritt voraus bleiben, Sicherheitsverletzungen verhindern und Ihre Investitionen in Technologien und Sicherheitsmaßnahmen bestmöglich nutzen.

Die drei Prinzipien einer modernen Identity-Strategie

Nachdem wir aufgezeigt haben, warum ein Identity-zentrierter Sicherheitsansatz wichtig ist, sehen wir uns nun die praktische Seite an: Wie können Sie mit Ihrem Unternehmen die Identity-Management-Ziele erreichen?

Mit modernen, Cloud-nativen Identity-Lösungen lassen sich Fragmentierungsprobleme schnell beheben. Sie bieten zentrale Kontrollfunktionen und einheitliche Echtzeit-Transparenz zu allen Systemen und Anwendungen. Außerdem bieten sie IT- und Security-Teams die Möglichkeit, blinde Flecken zu beseitigen, Risiken zu identifizieren und schnell zu reagieren.

Dieser enorme Mehrwert lässt sich in drei Kategorien einteilen:

Vollständige Transparenz

Gewährleistet, dass keine Schwachstellen übersehen werden und unbeachtet bleiben

Leistungsstarke Orchestrierung

Gibt die Möglichkeit, bei einer potenziellen Sicherheitsverletzung in Echtzeit zu reagieren

Umfassende und starke Integrationen

Ermöglichen die vollständige Vernetzung Ihres Sicherheits- und Tech-Stacks

Wenn Unternehmen sich nach einer modernen Identity-Lösung umsehen, müssen sie eine Plattform wählen, die bei diesen drei Prinzipien hervorragende Leistung bietet.

Prinzip 1

Vollständige Transparenz

Die individuelle Verwaltung der Zugriffsberechtigungen für die verschiedenen Anwendungen und Systeme führt zu ausnutzbaren Sicherheitslücken und Zugriffsrichtlinien, die permanent von menschlichen Fehlern untergraben werden.

Eine moderne Identity-Lösung muss Ihren Teams die Möglichkeit bieten, die Bereitstellung und Entziehung von Zugriffsrechten zu zentralisieren und zu vereinfachen. Außerdem muss sie einen umfassenden Echtzeit-Überblick über alle Identity-bezogenen Bedrohungen in Ihrem Unternehmen bereitstellen – sowohl bei Verwaltungs- als auch bei Laufzeitprozessen. Damit werden sichere und nahtlose User Experiences für alle Mitarbeiter, Partner und Kunden gewährleistet.

Verwaltungsprozesse

- Governance-Tools für einen umfassenden Überblick über die Zugriffe auf alle Systeme und Anwendungen, inkl. granulare und automatisierte Funktionen für Provisionierung und Deprovisionierung
- Posture-Management-Tools zur vereinfachten Analyse und Überwachung von Sicherheits-schwachstellen und Kundenidentitäten im gesamten Unternehmen

Laufzeitprozesse

- Tools zur Verwaltung privilegierter Zugriffe, die hochprivilegierte Informationen besonders stark schützen, ohne unnötige Reibungspunkte für IT-Teams oder Endbenutzer zu schaffen
- Funktionen zur Echtzeit-Bedrohungsreaktion, die mit Automatisierung und unternehmensweiter Überwachung schnell und effektiv potenzielle Bedrohungen beheben

Checkliste der erforderlichen Funktionen

- ☐ Transparenz zu allen Bedrohungen in allen Systemen, Geräten und Kundenkonten
- ☐ Einbeziehung von Drittanbieter-Signalen aus dem gesamten Tech-Stack (zusätzlich zu Signalen direkt von Ihrem Identity-Anbieter) für umfassenden Echtzeitüberblick über Bedrohungen
- ☐ Automatische Scans Ihrer Tools und Evaluierung Ihrer Konfiguration basierend auf aggregierten Zero-Trust-Frameworks
- ☐ Proaktive Identifizierung von Schwachstellen und Sicherheitslücken, bevor sie ausgenutzt werden können
- ☐ Kontinuierliche Aufdeckung kritischer Konfigurations-fehler und Lücken, z. B. inkonsistente MFA-Durchsetzung, Account-Ausbreitung und schwache Kundenauthentifizierungsrichtlinien
- ☐ Automatische Provisionierung und Deprovisionierung, wenn Benutzer innerhalb des Unternehmens die Position wechseln oder sich das Kunden-risikoprofil ändert
- ☐ Bereitstellung von sicherem Zugriff auf hochprivilegierte Informationen mit der Möglichkeit, die Zugriffsrechte je nach Benutzer und Use Case anzupassen
- ☐ Erkennung nicht-menschlicher Identities und Definition granularer Berechtigungen, um die Angriffsfläche des Unternehmens zu reduzieren
- ☐ Integration mit HR-Software und Directories zur konsolidierten Verwaltung von Mitarbeiter-informationen und -berechtigungen
- ☐ Verknüpfung mit Kundenidentitäten zur Verwaltung und Absicherung von Kundenkonten im benötigten Umfang

Prinzip 2

Leistungsstarke Orchestrierung

Fragmentierte Sicherheitstechnologien generieren riesige Datenmengen zu Risiken und potenziellen Bedrohungen. Ohne ein Identity-bezogenes Tool, das diese Daten vereinheitlicht, analysiert und darauf reagiert, müssen Ihre Teams Protokolle durchsuchen und nachträglich herausfinden, welche Risiken sofortige Aufmerksamkeit erfordern. Das Ergebnis ist eine langsame Sicherheitsfunktion, die Echtzeit-Behebung unmöglich macht.

Eine moderne Identity-Lösung muss Ihrem Team Tools zur Verfügung stellen, die potenzielle Bedrohungen in Echtzeit erkennen und umgehend verhindern können. Zusätzlich zur umfassenden Transparenz, die auf der vorherigen Seite beschrieben wurde, benötigen Unternehmen Identity-Funktionen, die das *Verständnis und die Reaktion* auf die ganzheitlichen Transparenzdaten vereinfachen. Dadurch lassen sich Angriffsversuche abwehren, bevor echter Schaden entsteht.

Checkliste der erforderlichen Funktionen

- ☐ Vereinfachte Einrichtung automatisierter Behebungsprozesse
- ☐ Granulare Anpassung der Behebungsmaßnahmen basierend auf Risikofaktoren, Richtlinien und anderen Kontextdaten
- ☐ Auslösung robuster Reaktionen wie universelle Abmeldung (Universal Logout) zum Schutz vor potenziellen Sicherheitsverletzungen
- ☐ Konstante Kommunikation mit Phishing-resistenten Authentifizierungstools zur kontinuierlichen Verbesserung der Behebungsstrategie
- ☐ Durchführung von Gerätesicherheitsprüfungen während aktiver Sessions
- ☐ Proaktive Blockierung gefährlicher IP-Adressen
- ☐ Self-Service-Optionen für Mitarbeiter und Kunden mit Phishing-resistenter Faktorwiederherstellung für sichere und einfache User Experiences
- ☐ Kontinuierliche Erkennung von Bedrohungen nach der Benutzerauthentifizierung

Prinzip 3

Umfassende und starke Integrationen

Ihr Tech-Stack ist nur so leistungsstark wie die Vernetzung. Ohne die nahtlose Integration zwischen den Komponenten Ihres Tech-Stacks ist es unmöglich, Ihre Technologie- und Sicherheitsinvestitionen optimal zu nutzen und den vollen ROI zu erreichen.

Eine moderne Identity-Lösung muss alle Komponenten verknüpfen, um umfassenderes Risikomanagement und höhere Effizienz zu ermöglichen. Herstellerneutrale Identity-Plattformen unterstützen diesen Grad an Integration, ohne dass Ihre Entwicklungs- und IT-Teams mit kundenspezifischem Code arbeiten müssen.

Checkliste der erforderlichen Funktionen

- ☐ Nahtlose Integration mit Ihren wichtigen SaaS-Anwendungen, z. B. CRM, Produktivität, Zusammenarbeit, ERP und IT-Ablaufverwaltung
- ☐ Umfangreiche Identity-Sicherheitsfunktionen, die über einfache Provisionierung und einmaliges Anmelden (SSO) hinausgehen, um diese Anwendungen vor, während und nach dem Login zu schützen
- ☐ Integration mit Kernelementen Ihrer Sicherheitstechnologien für bessere Risikoüberwachung, Bedrohungserkennung und Behebungsmaßnahmen
- ☐ No-Code-Optionen für Entwicklungs- und IT-Teams zur einfachen Erstellung von Automatisierungsabläufen, die Anwendungsfunktionen auslösen
- ☐ Erweiterungsfunktionen, die kontinuierliche Konnektivität für weitere Anwendungen und Systeme gewährleisten, die Ihr Unternehmen in der Zukunft hinzufügen könnte

Vorteile einer einheitlichen Sicherheitsstrategie

Einheitliche Identity-zentrierte Sicherheit ist nicht nur ein Konzept, sondern bietet verschiedene greifbare Ergebnisse, die in Kombination messbare Vorteile ermöglichen. Dazu gehören der Schutz kritischer Assets, die Vereinfachung der alltäglichen Workflows und die Steigerung der Leistung für alle Geschäftsabläufe.

- Transparenz zu allen Identity-bezogenen Bedrohungen sowie Echtzeit-Behebung
- Vollständige Umsetzung zuverlässiger Zero-Standing/Least-Standing-Privilegien
- Bewährte Zero-Trust-Strategie
- Bessere Kontrolle über nicht-menschliche und Maschinen-Identities
- Bestmögliche Nutzung Ihrer Technologie- und Sicherheitsinvestitionen

Hier erfahren Sie mehr über die fünf wichtigsten Ergebnisse einer einheitlichen Sicherheitsstrategie.

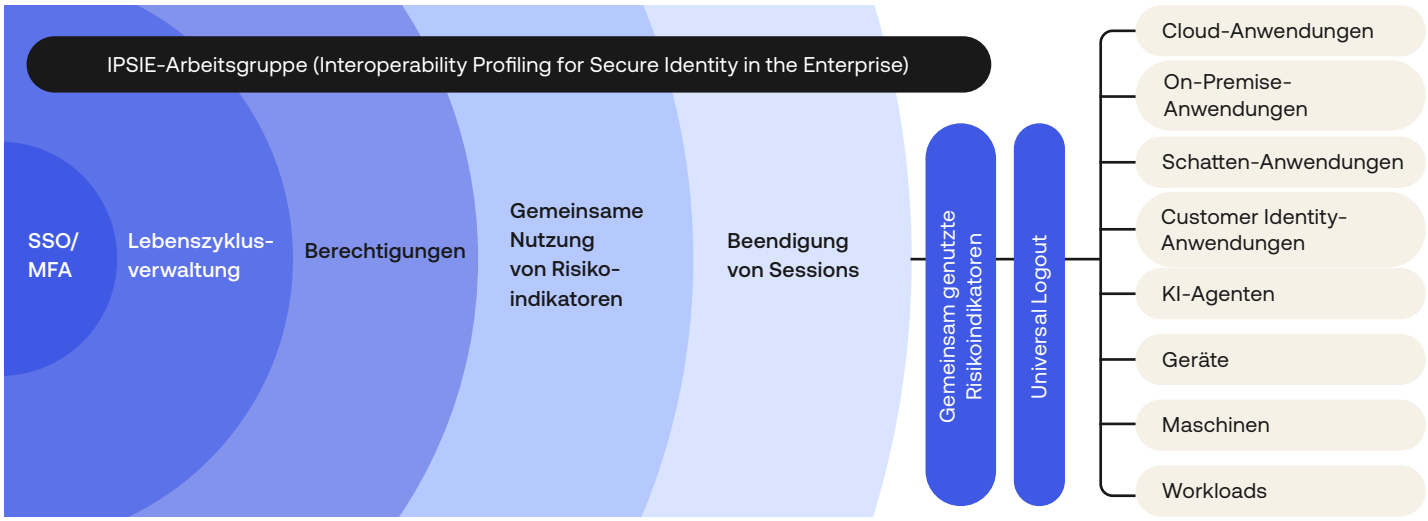
Der Weg zu Identity-zentrierter Sicherheit

Vollständig umgesetzte Identity-zentrierte Sicherheit unterstützt ein offenes Ökosystem, mit dem Unternehmen einfach, effizient und sicher alle erforderlichen Anwendungen, Systeme oder Tools erstellen sowie nutzen und dabei sicherstellen können, dass diese sicher sind und sich einfach verwalten lassen.

Damit sind Identity-Silos, kostenintensive und zeitaufwändige kundenspezifische Integrationen, Sicherheitslücken und blinde Flecken in Ihren IT- und Kundenumgebungen Geschichte. Stattdessen nutzen Sie einen leistungsstarken Tech-Stack, der grundsätzlich sicher und nahtlos ist.

Ein moderner Standard für Identity-Sicherheit

Die OpenID Foundation hat eine Arbeitsgruppe gebildet, die den Standard IPSIE (*Interoperability Profiling for Secure Identity in the Enterprise*) ausarbeitet, mit dem dieses Ziel in die Realität umgesetzt werden soll.



Als erster einheitlichen Identity-Sicherheitsstandard wird IPSIE die Voraussetzungen für ein vollständig integriertes Ökosystem schaffen, das den Anforderungen moderner Umgebungen gerecht wird und Ihnen wieder die Kontrolle in die Hand gibt.

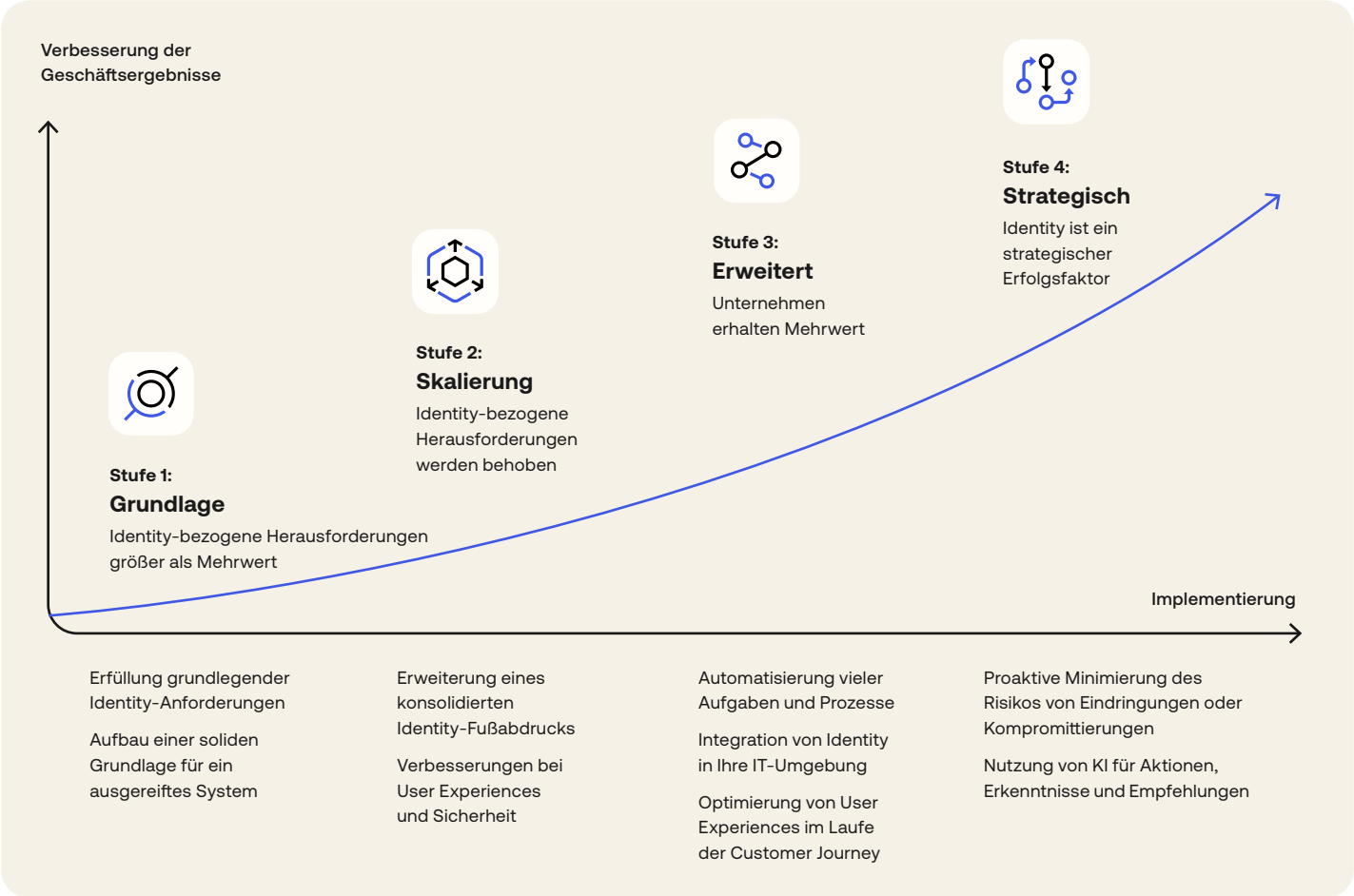
So erreichen Sie einen ausgereiften Identity-Ansatz:

Das Identity-Reifegradmodell von Okta

Die Modernisierung des Identity-Managements und die Vereinheitlichung der Sicherheitsstrategie ist für Security- und IT-Teams mit großem Aufwand verbunden. Zudem sind die Bedingungen nicht binär – vielmehr muss der Aufbau einer modernen Identity-Strategie im Rahmen einer auf Dauer angelegten Kampagne mit kontinuierlichen Verbesserungen erfolgen.

Deshalb hat Okta das Identity-Reifegradmodell entwickelt. Es stellt Unternehmen aus allen Branchen einen Rahmen zur Verfügung, der auf Expertenwissen und Branchen-Benchmarks basiert und Ihnen hilft, die komplexe Aufgabe zu bewältigen und Ihr Unternehmen voranzubringen.

Die jeweiligen Herausforderungen für Unternehmen hängen davon ab, wo sie sich gerade auf dem Weg zu ausgereiftem Identity-Management befinden. Das Identity-Reifegradmodell berücksichtigt diesen Umstand und gibt für jede Phase konkrete Hinweise zur optimalen Weiterentwicklung. Damit hilft das Modell enorm bei der Identifizierung von Prioritäten, der Bewertung des Fortschritts und der Erreichung der anvisierten Geschäftsergebnisse.



Mit einer sicheren Identity lässt sich alles schützen

Man kann es nicht genug betonen: Identity ist Sicherheit. Um Angreifern einen Schritt voraus zu bleiben und resiliente, wirksame Sicherheit zu implementieren, müssen Sicherheits- und IT-Verantwortliche ihre Identity-Lösung konsequent modernisieren und deren volles Potenzial nutzen.

Wenn Sie Ihre Identities schützen, schützen Sie die Zukunft Ihres Unternehmens: Sie schützen es vor der wachsenden Flut immer raffinierterer Bedrohungen und KI-gestützter Angriffsmethoden und sichern sich mit nahtlosen, automatisierten Sicherheits-, IT- und Kundenumgebungen Ihren Wettbewerbsvorteil.

Wenn Sie den Reifegrad Ihres Identity-Managements steigern und individuelle Empfehlungen von Okta-Experten erhalten möchten, können Sie hier mehr erfahren oder sich mit unserem Team in Verbindung setzen.

okta

Okta GmbH
Salvatorplatz 3
80333 München,
Germany
info_germany@okta.com
+49 (89) 2620 3329